Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, July 13th, 2016

Référence :ANSSI-CC-NOTE-19/1.0.1EN

APPLICATION NOTE

JILL "APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES" TABLE QUOTATION UPDATE

Application	:	From date of publication.
Circulation	:	Public.

COURTESY TRANSLATION

Version history

Version	Date	Modifications
1.0	13/07/2016	Creation
1.0.1	05/10/2016	Update to fix translation mistakes.

Pursuant to decree No. 2002-535 of 18th April 2002, this procedure has been submitted to the certification management committee, which delivered a favorable opinion.

This instruction is available online at the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1. Presentation

1.1. Subject of the note

This specific note adapts the "Access to TOE" quotation used during Common Criteria (CC) evaluations, for the technical domain "Hardware Devices with Security Boxes" within the French schema, based on [JIWG SB] document released on December 2015.

1.2. Reference

- [JIWG SB] : Joint Interpretation Library - Application of attack potential to hardware devices with security boxes, version 2.0, December 2015 (for trial use).

2. « A*ccess to TOE* » Quotation Section

The [JIWG SB] document has been created to meet the needs for product evaluations belonging to the category "hardware devices with security boxes". It is intended for evaluating products such as routers, smartcard secure readers, tachographs, HSM[1], etc.

However, this aforementioned document doesn't fully apply on equipment having notable physical and software protections. Indeed, section 2.2.5 "Access to TOE" of the document grants the following quotation:

Access to TOE (Samples)	Identification	Exploitation
Mechanical samples	1	1
Non functional samples	2	2
Fully functional samples	4	4

Where:

- *mechanical samples:* are non-functional samples that can still be used to study the external shielding conception (however the study of either the internal hardware structure or design is not possible);
- *non functional samples:* can be used to analyse the hardware structure of the TOE, such as the countermeasure implemented by the product;
- *fully functional samples*: operate with their external countermeasures deactivated; "open sample" belong to this category. These samples allow performing real simulations with the TOE.

With the actual quotation, a product having weak hardware protections (or easily bypassable), but for which the attacker needs a fully functional sample, can directly reclaim 8 points for its attack quotation. Which is not justified for such equipment.

To take into account such case, the following update of the quotation table is to be used (in bold in the following table).

[1] *Hardware Security Module.*

Access to TOE (Samples)		Identification	Exploitation
Mechanical samples	***with low hardware protection***	**Non applicable**	**Non applicable**
	with high hardware protection	1	1
Non functional samples	***with low hardware protection***	**1**	**1**
	with high hardware protection	2	2
Fully functional samples	***with low hardware protection***	**2**	**2**
	with high hardware protection	4	4

Where:

- *mechanical samples:* are non-functional samples that can still be used to study the external shielding conception (however the study of either the internal hardware structure or design is not possible);
- *non functional samples*: can be used to analyse the hardware structure of the TOE, such as the countermeasure implemented by the product;
- *fully functional samples*: are functional and unlocked, i.e. provided by the developer in a mode facilitating the implementation of the attacks. For example, the samples with their external technical countermeasures deactivated and open sample belong to this category;
- *with low hardware protection*: weak or easily bypassable hardware protections;
- *with high hardware protection:* strong and hardly bypassable hardware protections.